(19)日本国特許庁（ＪＰ） (12) 公開特許公報（A） (11)特許出願公開番号

特開平8－249239

(43)公開日 平成8年(1996)9月27日

(51)Int.Cl.⁶		識別記号	庁内整理番号	FI		技術表示箇所
G06F	12/14	320		G06F	12/14	320D
	15/78	510			15/78	510G
G06K	19/073			G06K	19/00	P

審査請求 有 請求項の数4 FD (全 4 頁)

(21)出願番号 特願平7－348757

(22)出願日 平成7年(1995)12月19日

(31)優先権主張番号 9415269

(32)優先日 1994年12月19日

(33)優先権主張国 フランス（FR）

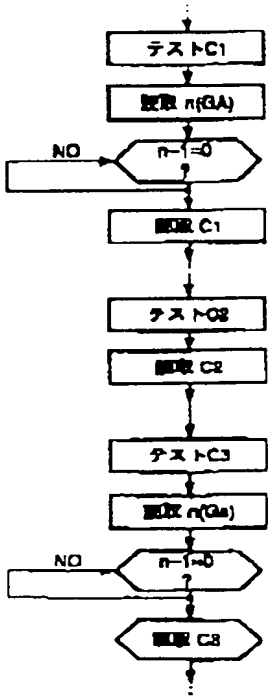
(71)出願人 591095720
エスジェーエス－トムソン ミクロエレクトロニクス ソシエテ アノニム
SGS－THOMSON MICROELECTRONICS SOCIETE ANONYME
フランス国 94250 ジャンティイ アヴニュ ガリエニ 7

(72)発明者 シルヴィー ヴィダル
フランス国 83310 プゥリエール ルカド 12

(74)代理人 弁理士 越場 隆

(54)【発明の名称】 集積回路の安全性を向上させるための方法および装置

(57)【要約】
【課題】 集積回路の安全性を向上させるための方法および装置
【解決手段】 少なくとも１つのマイクロプロセッサと異常な動作状態を検出するための１つまたは複数の安全性センサＣ１～Ｃ３とを備え、マイクロプロセッサによってアクセス可能なレジスタがそれぞれ対応するセンサの状態を記憶するように構成された集積回路の安全性を向上させるための方法が開示されている。この方法は、上記レジスタのうちの少なくとも１つについて、このレジスタを読み取る命令をマイクロプロセッサが受けた時に、ランダムな時間が経過してから読み取り動作を実行する。



【特許請求の範囲】

【請求項1】 少なくとも1つのマイクロプロセッサと異常な動作状態を検出するための1つまたは複数の安全性センサとを備え、マイクロプロセッサによってアクセス可能なレジスタがそれぞれ対応するセンサの状態を記憶するように構成されているような集積回路の安全性を向上させるための方法であって、上記レジスタのうちの少なくとも1つについて、このレジスタを読み取る命令をマイクロプロセッサが受けた時に、ランダムな時間が経過してからこの読み取りを行うことを特徴とする方法。

【請求項2】 マイクロプロセッサが上記レジスタを読み取らなければならない時はいつも、カウントループを初期化するためのランダムな値を引き出すようになされることを特徴とする請求項1に記載の方法。

【請求項3】 それぞれのレジスタに適用されることを特徴とする請求項1および2のいずれか一項に記載の方法。

【請求項4】 マイクロプロセッサに連結された擬似ランダムジェネレータを備えることを特徴とする請求項1～3のいずれか一項に記載の方法を実行するための装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、集積回路の安全性を向上させるための方法および装置に関するものである。本発明の方法は特に、あらゆる不正使用の試みに対する安全性を備えなければならない集積回路カードに適用される。これらは例えば、銀行関連の用途に使用されるカードまたは保護された場所へのアクセスをチェックするためのカードである。

【0002】このような用途のために、集積回路は少なくとも1つのマイクロプロセッサと秘密の情報要素を含む揮発性メモリとを備えている。情報要素は損傷されたり不正な動作によって外部に伝送されるようなことがあってはならない。

【0003】

【従来の技術】そのため、集積回路の動作を禁止しなければならないような異常な動作状態を検出するように構成された安全性センサが数多くある。そのように構成されたセンサには、過剰に低い周波数を感知するセンサ（周波数が低すぎると内部の動作をスパイし易くなる）、過剰に高い電圧または過剰に低い電圧を感知するためのセンサ（電圧が高すぎたり低すぎると、読み出しまたは書き込みされるメモリセルの内容が損なわれることがあるため）、過剰に高い温度または過剰に低い温度を感知するためのセンサ、あるいはデパッシベーションまたは光に対するセンサがある。

【0004】安全性センサはそれぞれ2進信号を発し、その信号の状態が正常な動作または異常な状態を表す。これら2進信号が集積回路を保護するために使用される。それら2進信号が直接、物理的な保護システム、例えばクロックのロックや、強制的な永久的初期化システムまたはその他のシステムを作動させてもよい。

【0005】それら2進信号はソフトウェア保護システムにおいて使用されてもよい。その場合、センサには記憶レジスタが接続される。マイクロプロセッサによって個々のレジスタがサンプリングされ、このマイクロプロセッサが個々の警報を考慮するか否かを決定し、状況に応じてどのような動作が行われるべきか（例えば再初期化、ロック、秘密データの破壊など）を決定する。レジスタは一般に単安定型のものである。警報が検出されるとレジスタが切り換わり、それらを初期の状態に再設定できるのは、マイクロプロセッサによって管理される安全になされた再初期化プロセスのみである。

【0006】センサはプログラム割込によって管理することができる。つまり、センサのレジスタが切り換わることによって、割込を管理するための対応するプログラムによってマイクロプロセッサが割込される。実際、割込信号はそれほど多くなく、その他の用途のために確保されている。

【0007】従って、センサのソフトウェアおよび順次動作を行うのが好ましいとされている。なぜならば、そのような動作は、用途に応じて程度の異なる安全性を確立することが可能となり、さらに間違った警報を管理することが可能となる。この方法は、システマティックなロック動作を行わずにすむためにより柔軟性が高い。つまり、センサの状態は各種の命令プログラムの実行中に逐次制御される。しかしながら、センサの状態の逐次使用は不正な用いられ方をする可能性があることに注意されたい。

【0008】つまり、もし不正を行おうとする個人がマイクロプロセッサによって逐次実行される各種の命令を見つけ出すことが可能であれば、この個人はシーケンス内で1つまたは複数のセンサの状態が読み取られる正確な瞬間を決定することができる。所定の動作（例えば電圧をオンすること、オペレータの命令を待つこと、読み取り動作やプログラミングあるいは識別コードの確認を実行することなど）について、これらは逐次命令であるので、この瞬間は常に同じである。

【0009】従って、センサの状態が読み取られる前またはちょうどその時に、確実に正常な状態が存在するようにして、これらの状態を直後に変更すればよい。マイクロプロセッサがセンサを読み取る時、対応する状態は正常である。従ってマイクロプロセッサは正常な動作を続ける。しかし実際には、動作状態は直後に変更されて「正常」ではなくなる。

【0010】従って、センサの状態の逐次使用は、一般の認めるところでは割込による動作よりも明らかに柔軟性が高いものの、安全性センサのチェックを回避するこ

とを可能にすることがわかってる。１つまたは複数のセンサの読み取り後、マイクロプロセッサが新たにチェックを行わない限り、その後の変化は、マイクロプロセッサにはわからない。ここで、これらのセンサを読み取り続けることは不可能である。なぜならプログラムの進行があまりにも遅くなってしまうからである。一般に、初期化時と、それぞれのサブプログラムについて少なくとも１回の適当な時間、例えばストラテジック動作の直前に読み取りが行われる。

【００１１】

【発明が解決しようとする課題】本発明の目的は、安全性センサのチェックプロセスを安全にすることにある。センサが読み取られる瞬間（単数または複数）を決定することを防ぐことができれば、マイクロプロセッサによって検出されることなく集積回路に異常な状態を与えることは、はるかに困難となろう。

【００１２】

【課題を解決するための手段】従って、少なくとも１つのマイクロプロセッサと異常な動作状態を検出するための１つまたは複数の安全性センサを備えている集積回路の安全性を向上させるための本発明による方法は、マイクロプロセッサによってアクセス可能なレジスタの各々が、それぞれ対応する安全性センサの状態を記憶するように構成されている。そして、少なくとも１つの上記レジスタについて、このレジスタを読み取る命令をマイクロプロセッサが受けた時に、ランダムな時間が経過したときこの読み取り動作を実行する。

【００１３】マイクロプロセッサは、上記レジスタを読み取らなければならない時はいつでも、カウントループを初期化するためのランダムな値を固定する。

【００１４】本発明はさらにそのような方法を実行するための、マイクロプロセッサに連結された擬似ランダムジェネレータを備えた装置に関するものである。以下、添付した図を参照しながらその他の特徴および利点をさらに詳しく説明する。以下の記載はなんら本発明を限定するものではない。

【００１５】

【発明の実施の形態】本発明によれば、図１に示すように、集積回路は、マイクロプロセッサ、プログラムメモリＲＯＭ、例えばE²ＰＲＯＭ型の不揮発性メモリおよび異常な動作状態を検出するための安全性センサを備えている。図に示した例では、それらは３個の安全性センサを備えている。つまり過剰に高い温度を検出するためのセンサＣ１、過剰に低い周波数を検出するためのセンサＣ２、および過剰に高い電源電圧を検出するためのセンサＣ３である。上記に示したように、その他のセンサを、デバッシベーションまたは過剰に低い温度または電圧などを検出するように構成させることが可能である。これらのセンサは一般に用いられるもので、当業者には広く周知である。従ってそれらの製造に関する詳細な説明は行わない。

【００１６】これらのセンサは、正常な動作または場合によっては警報を示す論理情報要素を発する。この情報要素は、マイクロプロセッサによって読み取られるレジスタ（図１ではセンサに統合されている）に記憶される。本発明によれば、集積回路はさらに、マイクロプロセッサからのコマンドを受けてランダム値ｎを与える擬似ランダムジェネレータＧＡを備えている。

【００１７】本発明によれば、初期化信号または外部からのコマンドに応答してサブプログラムを実行するマイクロプロセッサが、センサをテストせよという内部命令を受け取ると、マイクロプロセッサはまず初めに、カウントループを初期化するために擬似ランダムジェネレータに値ｎを要求する。数ｎがカウントされた後（マイクロプロセッサの命令サイクルの速度で）、マイクロプロセッサがセンサのレジスタを読み取って、異常事態管理用のプログラムに従ってそれを処理する。

【００１８】集積回路が複数のセンサを有する場合には、マイクロプロセッサがこの方法を全てのセンサに適用するか、そのうちのいくつかのみに適用する。マイクロプロセッサはこの方法を逐次テストされるセンサのうちの少なくとも最初のセンサに適用する。図２に示したセンサをテストするためのシーケンスの例では、この方法は図１のセンサＣ１およびＣ３に適用され、センサＣ２には適用されない。このようにして、逐次プログラムにランダムな時間が導入される。このことによってセンサが読み取られる時間を決定することが困難となる。しかしながらプログラムの継続時間は長くなる。

【００１９】従って、求められる安全性の程度によってプログラムの実行にとって許容可能な遅延を割り当てることが必要である。例えばテストすべきセンサの種類によってランダムな数字の幅を決定することが可能である。最大限の安全性が望まれる場合には、本発明の方法を集積回路の全てのセンサに適用する。

【図面の簡単な説明】

【図１】　本発明の装置に関連して使用される集積回路を示す概略図。

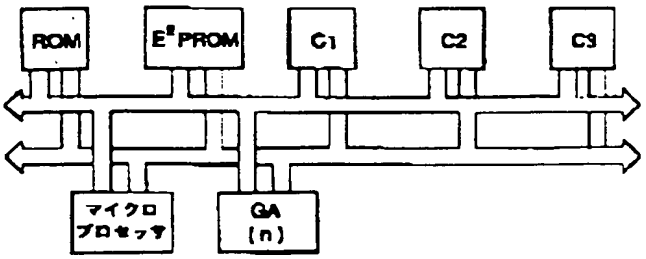
【図２】　本発明の方法に対応するフローチャート。

【符号の説明】

Ｃ１、Ｃ２、Ｃ３　センサ

ＧＡ　擬似ランダムジェネレータ

【図１】



【図２】